Journal of Technology Management & Innovation

Received August 22, 2010 / Accepted November 30, 2010 J. Technol. Manag. Innov. 2010, Volume 5, Issue 4

Examining the Relative Influence of Risk and Control on Intention to Adopt Risky Technologies

Sumeet Gupta[1], Heng Xu[2]

Abstract

For technologies such as electronic commerce, mobile payments, internet and mobile banking etc. customers are concerned about security issues that arise as a result of adoption of these technologies. However, in practice, we find that customers forgo their considerations of risk in the technology, if the benefits of using the technology overpower the risks involved in using the technology. Understanding their relative roles in technology adoption will help technology developers focus their efforts on either of them to improve technology adoption. Results of this study reveal that in adopting a technology, customers are guided more by the perception of control rather than by the perception of risk. Implications for theory and practice are discussed.

Keywords: mobile banking; security concerns; perceived risk; perceived control.

[1] Dept. of Business Administration. Shri Shankaracharya College of Engineering and Technology. Junwani, Bhilai, Dist – Durg (C.G.) India – 490 020. Tel: +91-788-600-0785 - fax: +91-788-229-1606. E-mail: sumeetgupta@ssitm.ac.in

[2] College of Information Sciences and Technology. Pennsylvania State University. 316h IST building. University Park, PA 16802,USA. Tel.: +1-814-867-0469 - fax: +1-814-865-6426. E-mail: hxu@ist.psu.edu

ISSN: 0718-2724. (http://www.jotmi.org)

Introduction

Every technology has some inherent risk. For example, using enterprise resource planning (ERP), while on the one hand, improves manufacturing efficiency; on the other hand, it increases the risk of making valuable information available indiscriminatingly. Similarly, while using internet banking makes banking efficient and easy, it increases privacy and security risks. Mobile banking brings banking on the move, but increases the risk of loss of security to unscrupulous people.

Although there are inherent risks in a technology, nonetheless individuals and organizations adopt technology when they feel that the benefits provided by the technology far outweigh the costs involved in adopting the technology (Davis, 1989; Davis, Bagozzi, and Warshaw, 1989; Dodds, Monroe, and Grewal, 1991). Even when the benefits do not outweigh the costs involved in the technology, the market forces (Teo, Wei, and Benbasat, 2003) influence organizations to adopt the technology. Firms adopt technology to remain competitive in the market. For example, in India only the top banks adopted ERP in the beginning (Year 2000). However, because of competition other banks also followed suit in order to remain competitive in the market. On an individual level also technology adoption increases due to word-of-mouth (I have to have it because others have it) and network effect. Many people adopt technology because of sheer fun of being recognized as the early adopter, while others wait for sufficient technology penetration before adopting the technology. These late adopters wish to see that all the major issues (technology related or otherwise) are resolved before they adopt the technology. In other words, they wish to be in sufficient control of the technology so that they are not affected by the risks involved in the technology.

Previous studies, have done extensive research on both perceived control (e.g., Mathieson, 1991; Pavlou and Fygenson, 2006; Taylor and Todd, 1995a) and perceived risk (e.g., Budnitz, 1998; Jarvenpaa and Leidner, 1999; Jarvenpaa, Tractinsky, and Vitale, 2000; Norberg, Horne, and Horne, 2007; Pavlou, 2003; Pavlou and Gefen, 2004) in technology adoption. These studies suggest that risk involved in a technology increase customers' concerns with security and thus slow down the adoption of the technology. Firms attempt to increase technology adoption by assuring them of various safety features that reduce risk in technology adoption (Xu et al., 2009). For example, encryption and authentication are some approaches that reduce the chances of failure due to risks in electronic commerce. Similarly, firms alleviate risks by adopting proper legal framework as well as obtaining certification from various agencies (such as eTrust) that certify the site to be secure / trustworthy.

A number of studies (e.g., Dinev and Hart, 2006; Wang et al., 2006; Xu, 2007a) argue that the rate of adoption can increase, if customers feel themselves in control of their transaction, even if the perceived risk in a technology is high. However, no empirical study has been conducted to substantiate this assertion. Therefore, this study attempts to study the relative role of risk and control in technology adoption. Specifically this study examines (i) how risk and control affect intention to adopt risky technology, and (ii) Which of the two, risk and control, exerts a stronger effect on intention to adopt? There is hardly any study that has attempted to study the relative role of risk and control in case of risky technologies. This study would therefore contribute to theory by examining their relative roles. This study would also contribute to practice by providing specific guidelines for improving technology adoption based on reducing risk or improving control.

Following section discusses literature review on risk and control. The related hypotheses are discussed in research model and hypothesis section. This is followed by research methodology and analysis of results. The final part of the report consists of the discussion of the results, their implication to research and practice and conclusions of the study.

Literature Review and Conceptual Background

Risky Technologies

Literature is replete with studies on adoption of risky technologies. Most of the studies on technology adoption use theory of reasoned action (Fishbein and Ajzen, 1975), technology adoption model (Davis, 1989; Davis, et al., 1989), innovation diffusion theory (Rogers, 1991), theory of planned behavior (Ajzen, 1991) and institutional theory (DiMaggio and Powell, 1983). Till 1990s, most of the technologies (such as excel software, computer) did not

involve significant risk for its users. Therefore, risk is not a major factor while considering their adoption. However, most of the later technologies, such as electronic commerce, e-payments, internet banking, mobile commerce, and mobile banking have inherent risks that impair their adoption.

Suh and Han (2003) assert that security is one of the most challenging problems faced by customers who wish to trade online because of the inherent vulnerabilities of the Internet. They argue that when a customer trades through the Internet, anyone from anywhere can access the information being transmitted. Bouwman et al. (2007) categories these barriers into physical (whether or not risky technology is physically accessible), cognitive (effort required in mastering the use of risky technology), affective (attitudes and motivation with regard to the use of systems, such as confidence, efficacy, and trust), economic (benefits and cost), social (cultural norms) and political (related to power and knowledge gaps). Table 1 presents some of the studies that identify the barriers to the adoption of risky technologies.

Authors	Risky Technology	Obstacles to Adoption
Sathye (1999)	Internet Banking	Security concerns and lack of awareness about Internet banking
Polatoglu and Ekin (2001)	Internet Banking	Perceived Risk
Liao and Cheung (2002)	Internet Based e-retail Banking	Security
Mallat (2007)	Mobile Payment	Premium pricing, Complexity, Lack of Critical mass, Perceived Risk
Lee et al. (2003)	3G Mobile Banking Services	Perceived Risk
Kleijen et al. (2004)	Mobile Games	Perceived Risk
Massoud and Gupta (2003)	Mobile Services	Security and Privacy, usefulness
Heres et al. (2004)	Mobile Internet	Technical infrastructure, available substitutions, price, design of technology, usability, availability of service, visibility and testability as technological barriers, and skills, capabilities and financial situation
Vrechoupoulos et al. (2003)	Mobile Commerce	Complicated use, lack of security, poor quality of service, high price for mobile access, inconvenience of devices and lack of personalization
Pagani (2004)	Mobile Multimedia	(Lack of) ease of use and navigation, limitation in bandwidth, cost, hardware and software functionality and privacy

Table 1. Barriers to Adoption of Risky Technologies

Table 1 reveals that user' security concerns and ease of use are some of the most common barriers to adopt risky technologies. Although the incidence of new technology has removed technological barriers, the affective barriers (such as perceived risk, security concerns and ease of use) are difficult to overcome. For example, banks overcome the (lack of) ease of use problems by educating the customers and reducing technological hassles. Security concerns, however, still pose a big hurdle barrier to overcome. A number of studies (e.g., Black, et al., 2002;

Chen and Barnes, 2007; Hamlet and Strube, 2000; Hernandez and Mazzon, 2007; Polatoglu and Ekin, 2001; Sathye, 1999; Tan and Teo, 2000) conducted on various risky technologies reiterate the importance of security concerns and find lack of security as a significant obstacle to the adoption of online banking. Roboff and Charles (1998) note that although customers' confidence in their bank is strong, yet their confidence in the technology is weak (Howcroft, et al., 2002). According to Daniel (1999), security concerns arise from the use of an open public network. Therefore, this study considers security concerns as an important factor in adoption of mobile banking.

Technology Risk

Risk is defined as the uncertainty resulting from the potential for a negative outcome (Havlena and DeSarbo, 1991) and the possibility of another party's opportunistic behaviour that can result in losses for one self (Ganesan, 1994; Yates and Stone, 1992). An individual's calculation of risk involves an assessment of the likelihood of negative consequences as well as the perceived severity of these consequences (Peter and Tarpey, 1975). In the context of risk technologies, perceived risk represents the subjective expectation of a loss or sacrifice in using the risky technology (Sweeney, et al., 1999). Following previous research (e.g., Featherman and Pavlou, 2003), this research defines perceived risk as *the expectation of losses associated with using a risky technology*.

As discussed earlier, risk is inherent in any technology. Risk may arise due to a number of reasons. Risk may arise due to system (e.g., system failure). Risk may also arise due to internet service provider failing to provide the needed service at a critical juncture. Risk may also arise due to the vendor (e.g., website in case of electronic commerce) misuses the personal information. There is also a risk of losing the password to unscrupulous people or the risk of someone stealing / hacking one's password. Finally, technology itself is a risky one, such as electronic commerce, which exposes people's personal information to a variety of risks. In this study, we are primarily interested in technology risks because other type of risks are not inherent to the technology under consideration and do not change with the technology. For example, the risks in using mobile banking will have risks inherent to mobile banking technology as well as the risks due to mobile service provider (service provider), mobile phone (risk due to system), risk due to theft (stealing of passwords by some stranger) and risk due to bank's misusing the information or not taking sufficient steps to contain the risk (risk due to vendor).

Perceived Control

Extensive research has been conducted on perceived behavioral control. Ajzen (1985) proposed the concept of perceived behavioral control in his theory of planned behavior. The theory of planned behavior is a widely used theory (e.g., Ajzen, 1991; Ajzen and Madden, 1986; Taylor and Todd, 1995a) for explaining customer adoption.

Perceived control reflects beliefs regarding the access to resources and opportunities needed to perform a behavior. The concept of perceived behavioral control is conceptually related to self-efficacy (Bandura, 1977). Perceived behavioral control refers to an individual's beliefs about the presence of factors that may facilitate or impede performance of the behavior (Ajzen, 1985). According to Ajzen (1991) and Taylor and Todd (1995b) perceived behavioral control encompass two components. The first component reflects the availability of resources (such as money and time) needed to engage in the behavior and the second component reflects the individual's self-confidence in the ability to conduct the behavior. This second component is termed as controllability and we are interested in this construct. This is because while time and money may not be a hindrance in the adoption of risky technologies, the controllability factor is. The lack of self-confidence in using a risky technology occurs on account of the fear of losing private information to unscrupulous people or any other breach of security.

A number of studies (e.g., Aldridge, et al., 1997; Bhimani, 1996; Furnell and Karweni, 1999; Gefen, 2000; Ratnasingham, 1998) have discussed the basic security-control requirements in risky technologies which may be divided into five categories, namely: authentication (communicating or transacting parties are who they claim to be), non-repudiation (neither of the party should be able to deny having participated in a transaction after the fact), confidentiality (warrants all communication between trading parties to be restricted to parties involved in transaction), privacy protection (ensures that personal information about customers collected from their electronic transactions is protected from disclosure

without permission) and data integrity (data under transmission is not created, intercepted, modified or deleted illicitly). These requirements are accomplished by various technologies, such as encryption, third-party certificates, digital signatures, and compliance with privacy policy (Aldridge, et al., 1997; Garfield and McKeown, 1997; Ratnasingham, 1998).

According to (Furnell and Karweni, 1999), although these advances have reduced the possibility of security breaches, customers do not adequately understand these security controls and the associated complex terminologies (Suh and Han, 2003). Moreover, it is not necessary (and also highly unlikely) that customers are aware of which technologies are implemented in risky technologies they use (Suh and Han, 2003). Most of the customers use risk technologies when they are aware of the vendor. For example, customers are able to adopt Internet banking because they are aware of the bank in the offline world. However, still there are so many security breaches, such as a phishing attacks. Therefore, it is not the implementation of security control by risky technologies that enhance adoption, but the consumers' awareness of these controls in risky technologies. Therefore, in this study we propose safety awareness as a surrogate to controllability aspect of perceived behavioral control. In other words, customers' awareness of safety would imply that customer has some control on the technology.

Research Model and Hypothesis

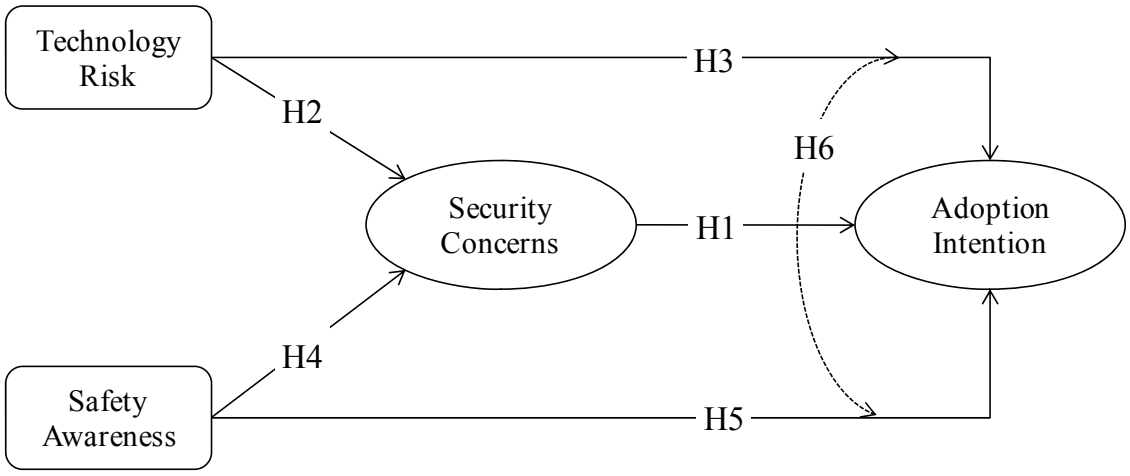


Figure 1. Research Model

Based on above discussion the research model of this study is shown in Figure 1. In this study we focus on mobile banking as a risky technology for several reasons. First, it is a risky technology. Secondly, it has been recently introduced in India. Thirdly, Indian banks are facing difficulties in increasing its adoption. Therefore, mobile banking provides a good avenue for our study.

Salisbury et al. (2001) define information security concerns as the buyer's beliefs about a seller's *inability* and *unwillingness* to safeguard their monetary information (such as credit card, social security numbers, user names and password and any information that may lead to financial consequences if stolen) from security breaches during transmission and storage. This research follows their definition for mobile banking adoption. As mobile banking is a highly personalized service as well as a global communication medium, it is exposed to many security vulnerabilities (Daniel, 1999). According to Daniel (1999), security concerns arise from the use of an open public network. Security concerns has been voiced (e.g., Black, et al., 2002; Chen and Barnes, 2007; Hamlet and Strube, 2000; Hernandez and Mazzon, 2007; Howcroft, et al., 2002; Polatoglu and Ekin, 2001; Sathye, 1999; Tan and Teo, 2000) as a significant issue in many areas related to mobile banking, such as internet banking. Security concerns relate to both hidden information and hidden action since buyers cannot ex ante select sellers who have the ability to

adequately safeguard their monetary information and who will ex post be willing and able to securely store and protect their monetary information from hackers (Pavlou, et al., 2007). Information security concerns lead to seller quality uncertainty, which stems from the buyers' difficulty in assessing a seller's ability and predicts the seller's willingness to safeguard monetary information. Buyers cannot thus accurately predict whether their monetary information will be appropriately safeguarded from security breaches and whether they will suffer financial problems in the future. Pavlou et al. (2007) assert that buyers must be confident in the seller's ability and willingness to safeguard their monetary information from security breaches during transmission and storage with authentication, encryption, and non-repudiation. The relationship between security concerns and purchase intention have been found to be significant (e.g., Salisbury, et al., 2001; Yang and Jun, 2002). Salisbury et al. (2001) showed that perceived information security is a stronger determinant of intention to purchase online than the website's perceived ease of use and usefulness. Similarly, Yang and Jun (2002) show that information security is considered the most critical concern for those who do not purchase online. Hence:

H1: Security concerns are negatively related to adoption intention

Perceived risk is referred to as the buyer's own subjective probability of suffering a loss in a transaction (Chiles and McMackin, 1996). In Cox's (1967) seminal model, perceived risk is conceptualized as involving two components, namely, uncertainty and adverse consequences. Recent conceptualizations (e.g., Mowen, 1992), define perceived risk in terms of expectation and importance of loss. Thus, perceived risk represents the subjective expectation of a loss or sacrifice in conducting transactions over mobile phone (Sweeney, et al., 1999). Following previous research (e.g., Featherman and Pavlou, 2003) this research defines perceived risk as *the expectation of losses associated with conducting banking transactions over mobile phone*. While security concerns deals with information security losses specific to the mobile banking, perceived risk is related to the general perception of uncertainty involved in trying out any innovation. Apart from theft and wilful negligence on part of sellers/banks, risk arises due to the inherent nature of the technology involved. For example, a customer may lose the amount due to transaction failure. Or the amount might get transferred to wrong account in spite of one being careful. Risk also arises due to losing the password to unscrupulous people beyond the control of banks. Moreover, a customer also develops risk perception based on their experience with other risky technologies, such as Internet banking. Roboff and Charles (1998) note that although customers' confidence in their bank is strong, yet their confidence in the technology is weak (Howcroft, et al., 2002). Therefore, if risk perception about technology is high, customers' security concerns about that technology will also be high.

H2: Technology risk is positively related to security concerns

As discussed earlier, perceived risk involves both uncertainty and adverse consequences. Salisbury et al. (2001) argue that the future states of the transaction could vary from a successful product fulfilment to any combination of numerous adverse possibilities. Buyers tend to overestimate the probability of potential losses, even if the probability of such losses is low (Kahneman and Tversky, 1979). Perceived risk has been considered as the detriment to exchange relationships (Rousseau, et al., 1998) and has also been shown to negatively influence consumer adoption of e-commerce (Pavlou, 2003). Perception of losses in a mobile transaction is likely to restrain the participation of buyers in the transaction. Therefore, when individuals perceive that there are risks in conducting banking transactions and that there will be negative consequences, they will be less likely to adopt mobile banking. Hence:

H3. Technology risk is negatively related to adoption intention.

Perceived control is considered as an important factor in the adoption of any risky technology. Although, perceived risk in a technology may be high, the rate of adoption can be increased if customers feel themselves in control of their transaction (Dinev and Hart, 2006; Wang, et al., 2006; Xu, 2007a). Perceived control refers to the customers feelings that he is under control of his transactions. To minimize losses, consumers place more importance in gaining control over transaction than on monetary or time savings (Koller, 1988). In general, consumers find it difficult to conduct transactions unless they have some assurance of safety of their transactions (Xu, 2007a). According to Margulis (2003), perceived control over the transactions conducted in electronic and mobile commerce plays an important role in alleviating

individual's concerns. For example, electronic commerce sites having trust and privacy seals are considered more secure as compared to sites without these seals. Similarly, when customers are assured of being in control of transaction over mobile phone through some password or other methods (e.g., law/act), they feel more in control of the transaction. In case of mobile banking control of transactions is ensured by incorporating safety features in the technology such as authentication and encryption. The control can also be ensured by incorporating transaction limits whereby a customer can conduct a transaction up to a specified limit only. Also, the relevant legislation governing these transactions also increase control perception of the customers about their transactions. To the extent a customer is aware about these safety features in conducting mobile banking transactions, to that extent he would be less concerned about security in the transactions. Hence:

H4: Safety awareness is negatively related to security concerns

When a customer is aware of safety features in the mobile banking transaction, he would be more willing to adopt mobile banking than when he is not aware of these safety features. Part of promoting mobile banking is to make customer aware about the safety features present in these transactions, so that they are more willing to adopt mobile banking. Accordingly, we propose that perceived control over transactions conducted over mobile phone is strongly related to individual's intention to adopt mobile banking. Hence:

H5. Safety Awareness is positively related to adoption intention

As discussed earlier, a number of studies (e.g., Dinev and Hart, 2006; Wang, et al., 2006; Xu, 2007a) argue that the rate of adoption can increase, if customers feel themselves in control of their transaction, even if the perceived risk in a technology is high. Although, intuitive there is no empirical test done to validate this assertion. Hence:

H6: Safety awareness has a stronger effect than technology risk on adoption intention

Research Methodology

As discussed earlier this study chose mobile banking as the targeted risky technology for testing the proposed model of this study. The data was collected using an online survey across potential users all over India. E-mails were sent to participants inviting them to the online survey. The survey was passed on to immediate contacts that in turn passed in on to their contacts. The questionnaire was administered to the respondents after introducing them to the process of mobile banking as launched by Indian banks.

For measuring constructs, this study adapted extant validated scales to the context of this study. Perceived risk was measured by adapting four items from Dinev and Hart (2006). Items for safety awareness were adapted from Xu (2007a). Items for intention to adopt were adapted from Dodds et al. (1991) and items for security concerns were adapted from (Pavlou, et al., 2007). Except the fourth item all other items were reverse coded. The survey instrument is shown in Appendix I.

The data obtained was cleaned for incomplete and missing responses, as well as cases where respondents answered all 7, all 1 or all 4. Such responses imply that the respondent has not read the questionnaire and/or is not making judgments. Final dataset consisted of 192 responses. Table 2 shows the demographic characteristics of respondents.

Data Analysis and Results

Exploratory factor analysis using VARIMAX rotation was conducted to assess the reliability and validity of the constructs. The factor analysis is shown in Table 3. All items loaded on the constructs they were intended to measure. The total variance explained by perceived risk, perceived control and intention to adopt was 80.49%. Cronbach's Alpha is greater than 0.7 for all constructs. Hence, the reliability and validity of the constructs is confirmed.

Item	Measure	Freq	%age	Mean	Std. Deviation
Age	<20	13	6.78	2.60	0.881
	20-29	79	41.15		
	30-39	50	26.04		
	>=40	34	17.71		
	Not Answered	16	8.33		
Gender	Female	38	19.79	----	----
	Male	138	71.87		
	Not Answered	16	8.33		
Income	< 1 Lakh	33	17.18	2.65	1.018
	1-2.99 Lakh	34	17.71		
	3-4.99 Lakh	71	36.98		
	>=5 lakhs	38	19.79		
	Not Answered	16	8.33		
Profession	Student	31	16.15	2.91	1.066
	Housewife	4	2.08		
	Employed	101	52.60		
	Self employed	29	15.10		
	Others	11	5.73		
	Not Answered	16	8.33		
	Total	**192**	**100**		

Table 2. Descriptive Statistics of Respondent Characteristics

To further analyse the data this study adopted 2-stage methodology of Structural Equation Modelling as recommended by Anderson and Gerbing (1988). Measurement model was tested to assess construct validity (convergent and discriminant validity) using LISREL 8.54. First, this study tested for unidimensionality. Unidimensionality means that for each measurement item, there should be one and only one underlying construct, i.e., the variance shared by items is not related to an unspecified latent variable. The test results reveal excellent fit (GFI=0.95; AGFI=0.92; Std. RMR=0.037; RMSEA=0.039).

This study then performed confirmatory factor analysis (CFA) to assess convergent and discriminant validity. Following criteria was used to assess the convergent and discriminant validity: Standardized loading > 0.7; Standardized loading > 2 x Standard error; significant t-statistic for each path; CR > 0.7 for each path; AVE > 0.5 for each path (Fornell and Larcker, 1981; Gefen, et al., 2000). The results of CFA analysis are shown in Table 4. Table 4 reveals that each standardized loading is greater than 0.7 and twice its standard error, each loading is significant, CR > 0.7for each path and AVE > 0.5 for each path. Thus, convergent validity is adequately established.

	μ	σ	1	2	3	4
INT1			**0.864**	0.212	0.031	0.217
INT2	4.55	1.59	**0.910**	0.239	0.026	0.105
INT3			**0.888**	0.216	0.027	0.147
SAFE1			0.209	**0.800**	-0.063	0.276
SAFE2	4.61	1.18	0.258	**0.841**	0.072	0.132
SAFE3			0.200	**0.813**	-0.020	0.225
SECU1			0.234	0.370	-0.243	**0.747**
SECU4	4.08	1.3	0.074	0.115	0.007	**0.888**
SECU5			0.251	0.295	-0.147	**0.815**
RISK1			0.075	-0.025	**0.896**	-0.092
RISK2	4.4	1.39	0.034	0.048	**0.882**	-0.170
RISK4			-0.031	-0.036	**0.820**	0.009
Total Eigen Value			4.84	2.48	1.32	1.01
% of Variance			40.33	20.68	11.04	8.44
Cumulative %			40.33	61.00	72.04	**80.49**

Table 3. Results of Factor Analysis using VARIMAX Rotation

Item	Std. loading	t-Value	CR	AVE	Alpha
INT1	0.86	14.69			
INT2	0.93	16.59	0.92	0.79	0.92
INT3	0.88	15.20			
SAFE1	0.82	13.02			
SAFE2	0.81	12.68	0.85	0.65	0.85
SAFE3	0.79	12.30			
RISK1	0.88	13.91			
RISK2	0.88	13.98	0.85	0.66	0.84
RISK4	0.65	9.59			
SECU1	0.90	15.26			
SECU4	0.68	10.38	0.87	0.70	0.87
SECU5	0.91	15.48			

Table 4. Confirmatory Factor Analysis using LISREL 8.54

	INT	SAFE	RISK	SECU
INT	**0.89**			
SAFE	0.508**	**0.81**		
RISK	0.040	-0.028	**0.81**	
SECU	-0.416**	-0.542**	0.224**	**0.84**

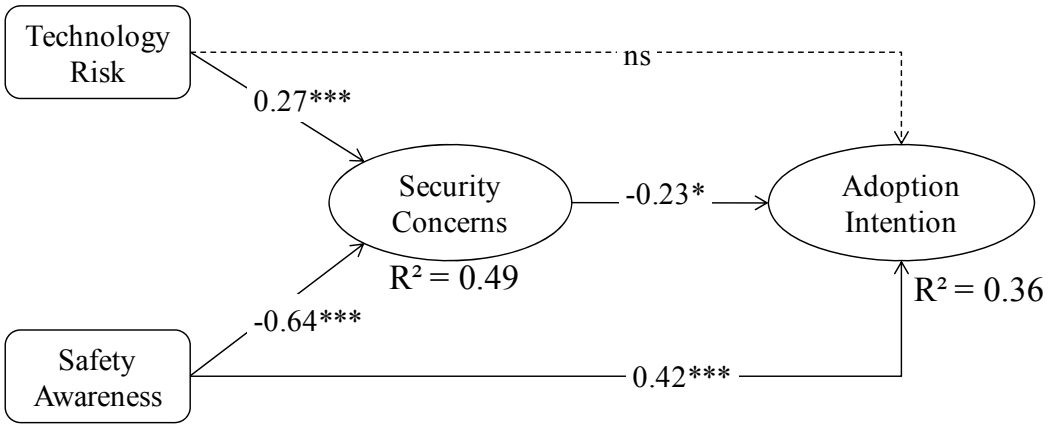
***: Correlation is significant at 0.01 level (2-tailed); Diagonal values are square of AVE of that construct*

Table 5. Correlation Between Latent Variables

To assess discriminant validity the square root of AVE of each construct is compared with the correlation between that construct and other constructs (Fornell and Larcker, 1981). Table 5 shows that the square root of AVE of each construct exceeds the correlation between that construct and other constructs. Thus, the discriminant validity of constructs in this study is established.

Hypothesis Testing (H1 to H5)

This study applied the following indices and standards to assess model fit following Hair et al. (1998): normed $\chi 2$ lower than 3.0, goodness-of-fit index (GFI) and normed fit index (NFI) greater than 0.90, adjusted goodness-of-fit index (AGFI) greater than 0.80, comparative fit index (CFI) greater than 0.90, and root mean square of approximation (RMSEA) lower than 0.08. The structural model had good fit indices (see Figure 2) and therefore, we can use standardized path coefficients for testing hypothesis. Safety awareness and security concerns significantly influence customers' intention to adopt mobile banking and explain 36% variance in adoption intention. Perceived risk and safety awareness significantly influence security concerns and explain 49% variance in security concerns. However, technology risk did not influence purchase intention significantly. Hence, all hypotheses were supported except H3.



Normed $\chi 2$=1.29, GFI=0.95, AGFI=0.92, NFI=0.97, CFI=0.99, RMSEA=0.039, Std. RMR=0.037

Figure 2. Structural Model

Since the strength of the relationship between security concerns and intention to adopt mobile banking was low, statistical power test was performed to make sure that the relationship was strong enough. To calculate statistical power G*Power software was used which is based on the F-test for multiple regression (Faul, et al., 2007). The statistical power of a research design is defined as the capacity of a design to detect the effect of the independent variable on the dependent variable, if one truly exists in the population. The higher the statistical power, the lower are the chances of committing Type II error (β). The acceptable minimum level for Type II error is four times that of Type I error (α=0.05), i.e., β = 4*0.05 = 0.20 in the field of Information Systems. This implies that the minimum acceptable statistical power of the model should be 0.80 (80%).

The statistical power depends on the sample size, the error probability (<5%), and the expected effect size (size of the path coefficients), and the number of predictors of the most complex construct (Cohen, 1988). In this study, the sample size was 192, error probability (0.05), effect size was 0.23 and number of predictors of the most complex construct were 3. Based on these values, the calculated statistical power obtained from G*Power software is 99.99%. This confirms that the relationship between security concerns and intention to adopt mobile banking is true.

Testing of Comparative effects (H6)

Since, the effect of technology risk on adoption intention is not significant we can safely conclude that safety awareness has a stronger effect on adoption intention as compared to technology risk. However, since the effect of technology risk (Beta = 0.14, p-value = 0.07) on adoption intention is insignificant on 95% confidence level, but significant at 90% confidence level. Therefore, within group constrained test (Byrne, 1998) was conducted to examine the comparative effects of technology risk and safety awareness on adoption intention. Figure 1 was taken as the base model. The equality constrained was imposed between the relationships: Technology Risk → Adoption Intention and Safety Awareness → Adoption Intention. If the χ^2 difference between the base model and the constrained model is insignificant (low fitting) for any particular group, it can be concluded that technology risk and safety awareness do not have significantly different effect on adoption intention. The results of the constrained test reveal that χ^2 difference is significant ($\Delta\chi^2$=6.65, Δdf = 1, p-value = 0.01). Since, the path coefficient for the relationship safety awareness → adoption intention is stronger than technology risk → adoption intention; safety awareness has a significantly stronger effect as compared to technology risk on adoption intention H6 is supported.

Discussion and Implications

The results of this study reveal interesting findings. All the hypotheses except H3 are significant. The results indicate that safety awareness and security concerns significantly influence a user's intention to adopt a risky technology. Moreover, the results suggest that the effect of control on adoption intention is stronger than the effect of risk on adoption.

The influence of technology risk on intention to adopt was insignificant, quite contrary to findings of numerous studies (e.g., Budnitz, 1998; Jarvenpaa and Leidner, 1999; Jarvenpaa, et al., 2000; Norberg, et al., 2007; Pavlou, 2003; Pavlou and Gefen, 2004) proposing risk as a major inhibitor to the adoption of risky technologies. This could be because customers look for ways and means to use the technology even when the risk is high. Therefore, when we consider the combined effect of safety awareness and technology risk, the influence of technology risk becomes insignificant. Another reason could be that we are only considering the technology risk and not other types of risk (i.e., due to system, vendor, service provider, theft) as considered by other studies. Thus, this study supports the assertion of earlier studies (e.g., Dinev and Hart, 2006; Wang, et al., 2006; Xu, 2007a) that rate of adoption can increase, if customers feel themselves in control of their transaction, even if the perceived risk in a technology is high.

Implications

This study reveals some interesting though niche findings. First, this is a unique empirical study in that it examines the relative effect of risk and control on adoption intention in case of risk technology. Secondly, this study provides empirical support to the assertion of previous studies (e.g., Dinev and Hart, 2006; Wang, et al., 2006; Xu, 2007a). Thirdly, the results of this study will be useful for service providers and vendors of risky technologies who can

improve and integrated controls in the technology as well as emphasize these controls when advertising their products. Consumers do not usually understand technical jargon, such as authentication, encryption etc. (Suh and Han, 2003) and therefore advertising as such may not improve the adoption of technology among end users. Therefore, technology developers and service providers can advertise their technology in a manner that is easily understandable by end users. Lastly, technology developers must understand the potential risks in using the technology and incorporate easy to use controls in their technology to overcome these potential risks. This would encourage and enhance the rate of technology adoption among potential users.

Conclusions and Limitations

Based on the assertion of a number of previous studies (e.g., Dinev and Hart, 2006; Wang, et al., 2006; Xu, 2007a), this study examined the relative role of risk and control on intention to adopt risky technologies. The results of this study revealed that control has a stronger effect on adoption intention than risk. This study thus marginally contributes to theory by examining their relative roles. The study also suggests that vendors or service providers of risky technology will be able to enhance adoption if they make customers aware of the controls they use to overcome the inherent risk of the technology. Even when the vendors / service providers of these risky technologies emphasize on controls used in the technology, the technical jargon used therein can be understood only by techies. They should rather emphasize safety features from a layman's perspective.

Despite our best endeavors, we acknowledge our limitations in conducting this study. First, the study was limited by time and resources. Respondents were quite unwilling to fill the survey form online and we had no provision for providing them suitable incentives for their support to us. May be from next surveys we will attempt to have some incentives for respondents in our studies. Secondly, our study was limited by the resources available in terms of contacts. We had to contact respondents through snowball sampling which may not be always the correct method for sampling respondents.

We explicitly focused on security concerns in this study and excluded privacy considerations because the service being offered is largely push based and requires less concern about privacy. However, future research can examine other facts of risk consideration. Using the groundwork laid down in this study, future research could contribute significantly to extending our theoretical understanding and practical ability to foster Mobile banking adoption.

References

AJZEN, I. (1985). From intentions to actions: A theory of planned behaviourz. In: Kuhl, J., Beckmann, J. (Eds.), *Action control: From cognition to behaviour*. Springer Verlag, New York. pp. 11-39.

AJZEN, I. (1991). The Theory of Planned Behaviour. *Organizational Behaviour and Human Decision Processes*, 50(2), 179-211.

AJZEN, I., Madden, T.J. (1986). Prediction of Goal-Directed Behavior: Attitudes, Intentions, and Perceived Behavioral Control. *Journal of Experimental Social Psychology*, 22(5), 453-474.

ALDRIDGE, A., White, M., Forcht, K. (1997). Security considerations of doing business via the Internet: Cautions to be considered. *Internet Research: Electronic Networking Applications and Policy*, 7(1), 9-15.

ANDERSON, J.C., Gerbing, D.W. (1988). Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach. *Psychological Bulletin*, 103 (3), 411-423.

BANDURA, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191-215.

BHIMANI, A. (1996). Securing the commercial Internet. *Communications of the ACM*, 39(6), 29-35.

BLACK, N.J., Lockett, A., Ennew, C., Winklhofer, H., McKechnie, S. (2002). Modeling consumer choice of distribution channels: an illustration from financial services. *International Journal of Bank Marketing*, 20(4), 161-173.

BOUWMAN, H., Carlsson, C., Molina-Castillo, F.J., Walden, P. (2007). Barriers and drivers in the adoption of

current and future mobile services in Finland. *Telematics and Informatics*, 24(2), 145-160.

BUDNITZ, M.E. (1998). Privacy protection for consumer transactions in electronic commerce: why self-regulation is inadequate. *South Carolina Law Review*, 49(1), 847-886.

BYRNE, M.B. (1998). *Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS: Basic Concepts, Applications, and Programming*. Lawrence Erlbaum Associates, Mahwah, New Jersey.

CHEN, Y.H., Barnes, S. (2007). Initial trust and online buyer behaviour. *Industrial Management and Data Systems*, 107(1), 21-36.

CHILES, T.H., McMackin, J.F. (1996). Integrating variable risk preferences, trust, and transaction cost economics. *Academy-of-Management-Review*, 21(1), 73-99.

COHEN, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). Lawrence Erlbaum Associates, Hillsdale, New Jersey.

COX, D.F. (1967). *Risk Taking and Information Handling in Consumer Behavior*. Harvard University Press, Boston.

DANIEL, E. (1999). Provision of Electronic Banking in the UK and the Republic of Ireland. *International Journal of Bank Marketing*, 17(2), 72-82.

DAVIS, F.D. (1989). Perceived Usefulness, Perceved Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, September, 319-340.

DAVIS, F.D., Bagozzi, R.P., Warshaw, P.R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35, 982-1003.

DIMAGGIO, R.J., Powell, W.W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, 48(2), 147-160.

DINEV, T., Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61-80.

DODDS, W.B., Monroe, K.B., Grewal, D. (1991). The Effects of Price, Brand and Store Information on Buyers' Product Evaluations. *Journal of Marketing Research*, 28(3), 307-319.

FAUL, F., Erdfelder, E., Lang, A.G., Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39(2), 175-191.

FEATHERMAN, M. S., Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451-474.

FISHBEIN, M., Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Addison-Wesley, Reading, Massachusetts.

FORNELL, C.R., Larcker, D.F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18(1), 39-50.

FURNELL, S.M., Karweni, T. (1999). Security implications of electronic commerce: A survey of consumers and businesses. *Internet Research*: *Electronic Networking Applications and Policy*, 9(5), 372-382.

GANESAN, S. (1994). Determinants of Long-Term Orientation in Buyer-Seller Relationships. *Journal of Marketing*, 58(2), 1-19.

GARFIELD, M.J., McKeown, P.G. (1997). Planning for Internet security. Information Systems Management, 14(1), 41-46.

GEFEN, D. (2000). *Electronic commerce*: *The role of familiarity and trust, Omega: The International Journal of Marketing Science,* 28(6), 725-737.

GEFEN, D., Straub, D., Boudreau, M. (2000). Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice. *Communications of AIS*, 4(7), 2-76.

HAIR, J.F., Jr., Anderson, R.E., Tatham, R.L., Black, W.C. (1998). *Multivariate Data Analysis with Readings* (5th ed.). Prentice Hall, Englewood Cliffs, New Jersey.

HAMLET, C., Strube, M. (2000). Community Banks Go Online. *ABA Banking Journal's* 2000 White Paper, 61-65.

HAVLENA, W.J., DeSarbo, W.S. (1991). On the Measurement of Perceived Consumer Risk. *Decision Sciences*, 22(5), 927-939.

HERES, J., Mante-Meijer, E., Pires, D. (2004). Factors influencing the adoption of Broadband Mobile Internet. In: Mante-Meijer, E., Klamer, L. (Eds.), *ICT Capabilities in Action: What People Do*. Cost Action, 269 Brussels.

HERNANDEZ, J.M.C., Mazzon, J.A. (2007). Adoption of internet banking: proposition and implementation of an integrated methodology approach. *International Journal of Bank Marketing*, 25(2), 72-88.

HOWCROFT, B., Hamilton, R., Hewer, P. (2002). Consumer attitude and the usage and adoption of home-based banking in the United Kingdom. *International Journal of Bank Marketing*, 20(3), 111-121.

JARVENPAA, S. L., Leidner, D. E. (1999). Communication and trust in global virtual teams. *Organization Science*, 10(6), 791-815.

JARVENPAA, S.L., Tractinsky, N., Vitale, M. (2000). Consumer Trust in an Internet Store. *Information Technology and Management*, 1(12), 45-71.

KAHNEMAN, D., Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263-292.

KLEIJNEN, M., de Ruyter, K., Wetzels, M. (2004). Consumer Adoption of wireless services: discovering the rules while playing the game. *Journal of Interactive Marketing*, 18(2), 51-61.

KOLLER, M. (1988). Risk as a determinant of trust. *Basic-and-Applied-Social-Psychology*, 9(4), 265-276.

LEE, M.S.Y., McGoldrick, P.F., Keeling, K.A.,Doherty, J. (2003). Using ZMET to explore barriers to the adoption of 3G mobile baking services. *International Journal of Retail and Distribution Management*, 31(6), 340-348.

LIAO, Z., Cheung, M.T. (2002). Internet-based e-banking and Consumer Attitudes: An Empirical Study. *Information and Management*, 39(4), 283-295.

MALLAT, N. (2007). Exploring consumer adoption of mobile payments: A qualitative study. *Journal of Strategic Information Systems,* 16(4), 413-432.

MARGULIS, S.T. (2003). Privacy as a Social Issue and Behavioral Concept. *Journal of Social Issues*, 59(2), 243-261.

MASSOUD, S., Gupta, O.K. (2003). Consumer perception and attitude toward mobile communication. *International Journal of Mobile Communications*, 1(4), 390-408.

MOWEN. J.C. (1992). The Time and Outcome Valuation Model: Implications for Understanding Reactance and Risky Choices in Consumer Decision-Making, In: Thomas, C.K. (Ed.), *Advances in Consumer Research,* Association for Consumer Research, Chicago, pp. 182-189.

NORBERG, P.A., Horne, D.R., Horne, D.A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-126.

PAGANI, M. (2004). Determinants of adoption of third generation mobile multimedia services. *Journal of Interactive Marketing*, 18(3), 46-59.

PAVLOU, P.A., Liang, H.G., Xue, Y.J. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal–Agent Perspective. *MIS Quarterly*, 31(1), 105-136.

PAVLOU, P.A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), pp. 101-134).

PAVLOU, P.A., Gefen, D. (2004). Building Effective Online Marketplaces with Institution-Based Trust. *Information Systems Research*, 15(1), 37-59.

PETER, J.P., Tarpey, L.X. (1975). A Comparative Analysis of Three Consumer Decision Strategies. *Journal of Consumer Research*, 2(1), 29-37.

POLATOGLU, V.N., Ekin, S. (2001). An empirical Investigation of the Turkish consumers. Acceptance of internet banking services. *International Journal of Bank Marketing* 19(4), 156-165.

RATNASINGHAM, P. (1998). The importance of trust in electronic commerce. *Internet Research: Electronic Networking Applications and Policy*, 8(4), 313-321.

ROBOFF, G., Charles, C. (1998). Privacy of financial information in cyberspace: Banks addressing what consumers want. *Journal of Retail Banking Services*, 20(3), 51-56.

ROGERS, E.M. (1991). The 'Critical Mass' in the diffusion of interactive technologies in organizations. In: Kraemer, K.L. (Ed.), *The Information Systems Research Challenge: Survey Research Methods*. Vol. 3, Harvard Business School Research Colloquium, Boston, pp. 245-271.

ROUSSEAU, D. M., Sitkin, S.B., Burt, R.S., Camerer, C. (1998). Not So Different After All: A Cross-Discipline View of Trust. *Academy of Management Review*, 23(3), 393-404.

SALISBURY, W., Pearson, R., Pearson, A., Miller, D. (2001). Identifying Barriers That Keep Shoppers off the World Wide Web: Developing a Scale of Perceived Web Security. *Industrial Management and Data Systems*, 101(4), 165-176.

SATHYE, M. (1999). Adoption of internet banking by Australian consumers: an empirical investigation. International *Journal of Bank Marketing*, 17(7), 324-334.

SUH, B., Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, 7(3), 135-161.

SWEENEY, J.C., Soutar, G.N., Johnson, L.W. (1999). The Role of Perceived Risk in the Quality–Value Relationship: A Study in a Retail Environment. *Journal of Retailing*, 75(1), 77-105.

TAN, M., Teo, T.S.H. (2000). Factors Influencing the Adoption of Internet Banking. *Journal of the AIS*, 1(5), 1-42.

TAYLOR, S., Todd, P.A. (1995a). Assessing IT Usage: The Role of Prior Experience. *MIS Quarterly*, 19(4), 561-570.

TAYLOR, S., Todd, P.A. (1995b). Understanding information technology usage: A test of competing models, *Information Systems Research*. 6(4), 144-177.

VRECHOUPOULOS, A., Constantiou, I., Sideris, I., Doukidis, G.,Mylonopoulos, N. (2003). The critical role of consumer behaviour research in mobile commerce. *International Journal of Mobile Communications*, 1(3), 329-340.

WANG, Y.S., Lin, H.H., Luarn, P. (2006). Predicting consumer intention to use mobile service. *Information Systems Journal*, 16(2), 157-179.

XU, H. (2007a). The Effects of Self-Construal and Perceived Control on Privacy Concerns. Paper presented at the *Proceedings of the 28th Annual International Conference on Information Systems (ICIS 2007)*, Montréal, Canada.

XU, H. (2007b). Privacy Considerations in the Adoption of Location-Based Services: A Psychological Control Perspective. Paper presented at the *67th Annual Meeting of the Academy of Management*, Philadelphia, PA.

YANG, Z., Jun, M. (2002). Consumer Perception of e-Service Quality: From Internet Purchaser and Non-Purchaser Perspectives. *Journal of Business Strategies*, 19(1), 19-41.

YATES, J.F., Stone, E.R. (1992). Risk appraisal. In: Yates, J.F. (Ed.), *Risk-taking behaviour*. John Wiley and Sons, Chichester, England, pp. 49-85.

Appendix I. Survey Instrument

Construct	Item	Question Wording	Source
Intention to Adopt Mobile Banking	INT1	I plan to subscribe to Mobile Banking Service in near (within next six months) future	Dodds et al. (1991)
	INT2	I intend to subscribe to Mobile Banking Service in near (within next six months) future	
	INT3	I predict I would subscribe to Mobile Banking Service in near (within next six months) future	
Security Concerns	SECU1	I would feel secure in providing sensitive information (e.g., bank account information) for conducting Mobile Banking transactions (Reverse Coded)	Pavlou et al. (2007)
	SECU4	The security issue of sensitive information will be a major obstacle to my conducting transactions over Mobile Phone	
	SECU5	Overall, Mobile Banking is safe for conducting Mobile Banking Transactions (Reverse Coded)	
Technology Risk	RISK1	It is risky to use Mobile Banking services	Dinev and Hart (2006)
	RISK2	There is high potential for security loss associated with using Mobile Banking Services	
	RISK4	My savings would be in jeopardy if I use Mobile Banking Services	
Safety Awareness	SAFE1	Banks are taking appropriate measures for safety of account information	Xu (2007b)
	SAFE2	A consumer protection act is in place to provide legal framework for transactions conducted over Mobile phones	
	SAFE3	RBI has issued specific guidelines for conducting mobile banking services all over the country	